UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/528,456	03/17/2000	Martin Kienzle	YOR000028US1	4380

7590 04/05/2004

Frank Chau Esq
F. Chau & Associates LLP
1900 Hempstead Turnpike
Suite 501
East Meadow, NY 11554

EXAMINER	
BOWES, SARA E	

ART UNIT	PAPER NUMBER
2136	6

DATE MAILED: 04/05/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/528,456	KIENZLE ET AL.	
	Examiner	Art Unit	
	Sara Bowes	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *1/9/04*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/17/00*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

Claims 1-34 are pending in this Office Action.

Applicant's arguments filed January 9, 2004 have been fully considered but they are not persuasive.

Rejections

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

Claims 1, 2, 6-13, 16-20, 22-26, 28-31, 33, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ichikawa to U.S. Patent 5,872,846 in view of Orrin to U.S. Patent 6,011,849.

Referring to claim 1, 20, and 33 Ichikawa teaches a system and method comprising a server [see Figure 5, Sender, 502] coupled to a transmission link for providing a data stream to at least one client [see Figure 5, Receiver, 516] over the transmission link [see Figure 5, Transmission], the data stream being segmented into units, the server including a scrambler for encrypting at least one first unit using an encryption key [see Figure 5, Encryption and Receiver's Public key, 508].

Ichikawa does not teach a system or method of a server comprising a steganographic unit for embedding the encryption key into at least one second unit for

the data stream such that steganographic information is needed by the client to determine the encryption key and decipher the data stream.

However, Orrin does teach a system and method of a server comprising a steganographic unit for embedding the encryption key into at least one second unit [see Figure 4, and column 4, lines 45-47].

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ichikawa to include the steganographic teachings of Orrin. Namely, inserting a steganographic unit in the "sender terminal" 502 of Figure 5 [see Ichikawa]. One of ordinary skill in the art would have been motivated to modify Ichikawa as above for the purpose of improving the security of the encrypted data to be transmitted over an unsecured communication line.

Referring to claim 2, Ichikawa as modified by Orrin teaches a steganographic unit employing a steganographic masking algorithm [see column 4, lines 39-40 of Orrin].

Referring to claim 4, Ichikawa as modified by Orrin teaches steganographic unit encrypts the at least one second unit [see column 4, lines 52-63 of Orrin].

Referring to claims 5, 11, 17, 23, and 29, Ichikawa as modified by Orrin teaches at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key [see column 8, lines 44-58 of Orrin].

Referring to claims 6, 12, 18, 24, and 30, Ichikawa as modified teaches a transmission link including the Internet [see column 3, lines 30-32].

Referring to claims 7, 13, 19, 25, and 31, Ichikawa as modified teaches at least one of the client and the server including a memory storage device [see Figure 5,

Receiver's Public Key, 508 and Receiver's Private Key, 520 and column 5]. In order for the sender [server] and receiver [client] to use the private and public keys of the receiver there must be a memory device to store the keys.

Referring to claims 8, 26, and 34, Ichikawa teaches a system and method comprising a client system coupled to a transmission link for receiving a data stream to at least one server over the transmission link, the data stream being segmented into units, the client system including a descrambler for descrambling at least one second unit which was encrypted in accordance with the encryption key before transmission from the server [see Figure 5, Decryption and Receiver's Private Key, 520].

Ichikawa does not teach a system or method of a client comprising:

- a key extractor for extracting an encryption key steganographically hidden in at least one first unit in the data stream received from the server such that steganographic information is needed by the client to determine the encryption key; and
- a decoder coupled to the key extractor and the descrambler for reassembling the data stream such that all of the units of the data stream are needed to decipher the data stream.

However, Orrin does teach a system and method of a client comprising:

- a key extractor for extracting an encryption key steganographically hidden in at least one first unit in the data stream received from the server such that steganographic information is needed by the client to determine the encryption key [see column 9, lines 13-16]; and

- a decoder coupled to the key extractor and the descrambler for reassembling the data stream such that all of the units of the data stream are needed to decipher the data stream [see column 9, lines 16-19].

Also refer to column 9, lines 34-42 of Orrin for further explanation.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ichikawa to include the key extractor and the decoder of Orrin. Namely, inserting the key extractor and the decoder in the "receiver terminal" 516 of Figure 5 [see Ichikawa]. One of ordinary skill in the art would have been motivated to modify Ichikawa as above for the purpose of providing a higher level of secure to encrypted data being transmitted over an unsecured transmission line.

Referring to claim 10, Orrin as modified teaches hiding the encryption key is also steganographically hidden in the at least one second unit [see Figure 4 and column 4, lines 45-55].

Referring to claims 16, 22, and 28, Orrin as modified teaches the step of steganographically embedding portions of the encryption key in the at least one first unit [see column 8, lines 44-58].

Claims 3, 9, 14, 15, 21, 27, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ichikawa in view of Orrin, and further in view of Katta et al.

Referring to claims 3, 9, 15, 21, and 27, Ichikawa and Orrin teach all limitations of the aforementioned claims except for the data stream including a transmission order, which alternates between first units and second units.

Katta et al. disclose a data stream including a transmission order, which alternates between first units and second units [see Figure 3 and column 3, lines 16-19].

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Ichikawa and Orrin to include the transmission order of Katta et al. Namely, inserting a multiplexer at the output of the "sender terminal" 502 of Figure 5 [see Ichikawa]. One of ordinary skill in the art would have been motivated to modify Ichikawa and Orrin as above for the purpose of improving the security of the data stream by separating the data into the data packets making the entire program [movie, music files, etc.] more difficult to decrypt.

Referring to claims 14 and 32, Ichikawa teaches a method comprising:

- providing data to be transmitted over a link [see Figure 5, Transmission];
- scrambling at least one first unit by encrypting the at least one first unit using an encryption key [see Figure 5, Encryption and Receiver's Public key, 508]; and
- descrambling at least one first unit which was encrypted in accordance with the encryption key [see Figure 5, Decryption and Receiver's Private Key, 520].

Ichikawa does not teach a method comprising:

- steganographically embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by a client to determine the encryption key and decipher the data;
- extracting the encryption key steganographically embedded in the at least one second unit in the data stream;

- reassembling the data steam at the client such that all of the units of the data stream are needed to decipher the data stream.

However, Orrin does disclose a method comprising:

- steganographically embedding the encryption key into at least one second unit for the data stream such that steganographic information is needed by a client to determine the encryption key and decipher the data stream [see Figure 4, and column 4, lines 45-47];
- extracting the encryption key steganographically embedded in the at least one second unit in the data stream [see column 9, lines 13-16];
- reassembling the data steam at the client such that all of the units of the data stream are needed to decipher the data stream [see column 9,lines 16-19].

However, neither Ichikawa nor Orrin explicitly teach segmenting the data into units for a data stream to be transferred over the line.

Katta et al does teach segmenting the data into units for a data stream to be transferred over the line [see Figure 3 and column 3, lines 16-19].

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the teachings of Ichikawa to include the teachings of Orrin. Namely combining the subsystems of claims 1[the server system] and 8 [the client system]. One of ordinary skill in the art would have been motivated to modify Ichikawa as above for the purpose of producing a secure, compatible server client network.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined teachings of Ichikawa and Orrin to include the teaching of Katta et al. Namely, inserting a multiplexer at the output of the "sender terminal" 502 of Figure 5 [see Ichikawa]. One of ordinary skill in the art would have been motivated to modify Ichikawa and Orrin as above for the purpose of improving the security of the data stream by separating the data into the data packets making the entire program [movie, music files, etc.] more difficult to decrypt.

Response to Arguments

Applicant argues:

1. Ichikawa does not teach or suggest 'encrypting at least one first unit using an encryption key" and " embedding the encryption key into at least one second unit for the data stream" of claims 1, 20, 33
2. Orrin does not teach applying an encryption key to a first unit of data stream and a steganographic method to a second unit of the data stream. Of claims 1, 20, 33
3. Orrin does not teach that the encryption key is extracted from a first unit of the data stream steganogrphically, wherein the encryption key is used to decrypt a second unit of the data stream.
4. Orrin does not teach a first unit and second unit of the data stream, essentially as claimed in claims 8, 26, and 34.

5. Orrin does not teach or suggest "wherein the at least one first unit and the at least one second unit are encrypted and each carries a portion of the encryption key" as claimed in claims 5, 11,17, 23, 29.
6. Orrin does not teach that the encryption key is steganographically embedded or hidden in an encrypted data stream.
7. Orrin does not teach or suggest a first and a second unit of the data stream, much less "steganographically embedding the encryption key into at least one second unit for the data stream" as claimed in claims 14 and 32.
8. Orrin does not teach applying an encryption key to a first unit of the data stream and a steganographic method to a second unit of the data stream.

Referring to argument 1., examiner disagrees with applicant. Ichikawa does disclose encrypting data by a sender using a key [ABSTRACT, lines 3-4]. Ichikawa also discloses encrypting the key bye the sender using an asymmetric encryption algorithm and transmitting it to the user. The authorized user decrypts the encrypted key using the encryption algorithm and then uses the key to decrypt the encrypted data. As stated in the rejection for claims 1, 20, and 33, Ichikawa does not disclose a steganography method. Orrin discloses the steganography method/system. Orrin embeds the key into a secondary data stream to be sent to the user to then be extracted and used to decrypt the cyphertext [ABSTRACT, lines 5-6 and 8-12]. Thus, Ichikawa combined with Orrin do disclose "encrypting at least one first unit using an encryption key" and "embedding

the encryption key into at least one second unit for the data stream", referring to claims 1, 20, and 33.

Referring to arguments 2-4 and 7-8, examiner disagrees with applicant. The argument set forth for argument 1., of the combined teachings of Ichikawa and Orrin disclose the limitations claims 1-34.

Referring to arguments 5., Orrin teaches embedding a portion of the key into first and second units [column 4, lines 65-67]. The present argument combined with Ichikawa discloses all limitations of claims 5, 11, 17, 23, and 29.

Referring to argument 9., examiner disagrees with applicant. Orrin does disclose applying an encryption key to a first unit and a steganographic method to a second unit of the data stream [ABSTRACT, lines 3-8].

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sara Bowes whose telephone number is 703-305-0326. The examiner can normally be reached on 7:30-4:00, Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

seb
3/31/2004